IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Axel Busboom	§ §	Group Art Unit:	2431
Application No	10/551,855	§ §	Examiner:	CHAI, LONGBIT
Filed:	07/26/2006	§ §	Confirmation No:	6153

Attorney Docket No: P16731-US1
Customer No.: 27045

For: METHOD FOR PROVISION OF ACCESS

CERTIFICATE OF MAILING OR TRANSMISSION
I hereby certify that this correspondence is being deposited with the United Sates Postal Service with sufficient postage for First class or Express mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or being facsimile transmitted to the USPTO at (571) 273-8300 or being transmitted via EFS-Web on the date indicated below.

Date: May 25, 2010

Signature: /Pamela C. Shultz/
Pamela C. Shultz

Via EFS-Web

Mail Stop AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Examiner:

DECLARATION UNDER 37 C.F.R. § 1.132

I, Daniel Catrein, hereby state that:

1. I am an expert in the field of information security.

2. I am a Senior Research Engineer at Ericsson in Aachen, Germany.

3. I was in 2007 with the German Federal Office for Information Security (BSI) in Bonn, Germany, I held an engineering position at the department for the development of cryptographic systems.

4. I received my Ph.D. in Communications Engineering from Rheinisch-Westfälische Technische Hochschule Aachen University in 2007.

5. While attending Rheinisch-Westfälische Technische Hochschule Aachen University, I held the position of Researcher at the Institute for Theoretical Information Technology (2004-2007) and the Institute of Stochastics (2001-2004).

6. My experience as a Senior Research Engineer at Ericsson, as an Engineer at the BSI and as a Researcher at Rheinisch-Westfälische Technische Hochschule Aachen University forms the basis for my opinion.

7. Examiner Chai asserted that "(a) any transformed random number / public key that can uniquely identify a user is qualified as part of a "principle identifier" of the user and (b) the user information (e.g., user public key, user random number and etc.) included in the access request query package / message is qualified as a principle." This assertion by Examiner Chai would only hold true if data providing entity has means to relate the data provided in the query package to the corresponding user, which is not the case for Eppstein, as detailed in the following.

8. Object of Eppstein is to provide to a user access to data from an information provider such that the user stays anonymous to the information provider.
P16731 object is to provide to a data requesting entity access to data that is related to a principal identifier. By providing the principal identifier to the data providing entity, the principal is known to the data providing entity in so far as the "principal identifier represents the principal towards the data providing entity".

9. According to Eppstein, the user makes a query Q with Q=relevant medical information of the user (e.g. symptoms, medical images, blood test results, history) in which information from which the user identity might be ascertained is redacted. The information provider receiving the query Q formulates a response R. Hence Q is related to R at the information provider. Thus, information at the information provider of

Eppstein has no relation to any user identity. In fact, information is not related to any particular user but to a query Q from which everything from which the user could be identified from has been redacted.

Further, according to Eppstein, for a formulated query, the public key of the user and the private key of the user are generated at the user equipment 12 "for the sole use of said formulated query" (see description and claim 1). The query contains the freshly generated public key of the user. No information at the information provided is related to this public key of the user in advance as the public key of the user is freshly generated for the sole purpose of this query. Furthermore, the public key is solely used for encrypting the response. To summarize, the public key of the user according to Eppstein cannot be used for identification purposes at all and is not used therefore! Note that the same holds true for the generated random number.

In P16731, the data is related to the principal identifier. Access to data that is related to a particular principal identifier is provided within the limits of the access specification for this particular principal identifier in the access granting ticket. Further, the principal identifier represents the principal towards the data providing entity, i.e, the data providing entity knows when receiving and processing an access granting ticket comprising a principal identifier the principal as represented by this principal identifier.

10. Further, I want to point out that the flow of Information and the roles of involved entities differ between Eppstein and P16731.

In Eppstein, the query is sent from the user equipment 12 to the public terminal 14 and from there to the information provider 18 which then posts the requested information to the public bulletin board 20 from which the user can access this information either from the public terminal 14 or from user equipment 12, in short

A) 12->14->18->20->14 or

B) 12->14->18->20->12

In P16731, the access granting ticket is sent from the principal entity (PE) to the data requesting entity (IRE) to the data providing entity (IPE) which provides access to the data according to the contents of the access granting ticket to the data requesting entity (IRE), in short

C) PE->IRE->IPE->IRE

Comparing B) with C), it is evident that no access to the information is provided to the public terminal 14, i.e. the public terminal 14 does not qualify for a data requesting entity to which access to the data is provided.

Comparing A) with C), the information is provided to the public terminal 14, however, the information is still encrypted and the public terminal 14 cannot access the information. Hence, also here the public terminal 14 does not qualify for a data requesting entity to which access to the data is provided.

11. I hereby declare that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true; and further, that these statements are made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001, Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Date: 25.5.2010

Daniel Catrein